SOPHOS

2020-10-13 08:10 CEST

Sju tips som säkrar IT-miljön i hemmet

Per Söderqvist, IT-säkerhetsexpert på Sophos har flera bra tips om hur man håller IoT-enheter och datorer säkra hemma. Något som är speciellt viktigt om hemmet också blivit arbetsplatsen.

– Det gäller att vara försiktig när man bygger sitt smarta hem. Med allt fler uppkopplade enheter och inte minst en ökad andel hemarbete ökar risken för att man blottar sig och bjuder in cyberkriminella som är ute efter pengar och information, kommenterar Per Söderqvist, säkerhetsexpert på Sophos.

Så här stänger du dörren för objudna gäster

De här sju tipsen hjälper dig att slå igen dörren för cyberkriminella. Samtliga

rör IoT-enheter i ditt hemnätverk och installationen av ditt nätverk i allmänhet.

1. Koppla ur. Behöver jag använda den här enheten online? Om inte, överväg att ta bort den från ditt nätverk. Eller se till att stänga av den när du inte använder den. Att bara koppla ur den från vägguttaget är ofta allt du behöver göra.

2. Uppdatera. Vet jag hur jag uppdaterar produkten? Om inte, ta reda på hur! Om leverantören inte kan försäkra dig om säkerhetsuppdateringar, överväg att byta till någon som gör det.

3. Se över säkerheten. Vet jag hur jag konfigurerar enheten? Se till att du vet vilka säkerhetsinställningar som är tillgängliga, vad de är avsedda för och hur du ställer in dem.

4. Ändra standardinställningarna. Hur ser standardinställningarna ut? Många IoT-enheter har fjärrsökningsfunktioner aktiverade för att kunna åtgärda fel. Det kan missbrukas. Samma sak gäller standardlösenord (som skurkarna definitivt känner till). Kontrollera och ändra eventuella standardinställningar – innan du kopplar upp enheten.

5. Dela klokt. Hur mycket information delar jag? Om enheten är ansluten till en onlinetjänst bör du bekanta dig med hur mycket data som delas och hur ofta. Du kan gärna dela med dig av data, men känn dig aldrig pressad att "maxa" inställningarna.

6. Använd separata nätverk. Kan jag dela upp mitt nätverk? Vissa hemroutrar låter dig dela ditt Wi-Fi i två nätverk som kan hanteras separat. Detta är användbart om du arbetar hemifrån eftersom det innebär att du kan placera dina privata IoT-enheter i ett gästnätverk och dina arbetsenheter som en bärbar dator på ett annat.

7. Rapportera problem. Vet jag vem jag ska vända mig till om det uppstår problem? Om du har tillgång till en IT-avdelning med teknisk support, se till att du vet var du ska rapportera något misstänkt. Fråga dem vilken information de vanligen behöver och ge den så tidigt som möjligt för att påskynda processen.

Om du bevakar säkerhetsfrågor och vill prata mer om IT-säkerhet i hemmet är du välkommen att kontakta Per Söderqvist, säkerhetsexpert på Sophos, telefon 0761-75 00 64 eller e-post per.soderqvist@sophos.com.

Sophos skyddar över 400 000 organisationer av alla storlekar i mer än 150 länder och är världsledande inom nästa generations cybersäkerhet. SophosLabs är en central del av verksamheten och består av ett globalt team av säkerhetsexperter som arbetar med att säkra klienter (bärbara datorer, servrar och mobila enheter) och nätverk med hjälp av moln- och AI-baserade lösningar. Sophos lösningar skyddar mot ständigt nya hot i form av bland annat gisslanprogram, skadlig kod, så kallade exploits, riktade attacker och nätfiske.

I molnplattformen Sophos Central finns en hel portfölj av produkter och tjänster, inklusive det avancerade klientskyddet Intercept X och brandväggen XG. Det ger en automatiserad, synkroniserad säkerhet och en helhetslösning som är tillgänglig via API:er. Sophos säljer sina produkter och tjänster via en global kanal med över 47 000 partner och Managed Service Providers (MSP). Företaget riktar sig också direkt till konsumenter med Sophos Home. Sophos har sitt huvudkontor i Oxford, England och är noterat på Londonbörsen under namnet ”SOPH”. Mer information finns på www.sophos.com

Kontaktpersoner

Per Söderqvist
Presskontakt
Team Leader Sales Engineer
Nordics and Baltics
Per.Soderqvist@Sophos.com
+46 (0) 76 175 00 64